IN THE CLAIMS:

Please amend the claims as follows:

1. (currently amended) A method comprising:

retrieving in a secure processing point separated from and arranged in communication with a personal device, a unique chip identifier from a read-only storage of an integrated circuit chip included in the personal device;

the secure processing point assembling a data package and loading the data package in the personal device for storage therein, the data package including at least one cryptographic key specific to the personal device;

receiving at the secure processing point, in response to storing the data package, a backup data package from the personal device, which backup data package is the data package encrypted with a unique secret chip key stored in a tamper-resistant secret storage of the integrated circuit chip included in the personal device;

associating the unique chip identifier with the received backup data package; and

storing the backup data package and the associated unique chip identifier in a permanent public database separated from the personal device;

wherein the secure processing point further performs:

associating a unique device identity with the unique chip identifier;

signing the associated unique device identity and unique chip identifier~~, with~~ using a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, thereby generating a certificate for the unique device identity;

storing the certificate in the personal device; and

storing in the permanent public database, the unique device identity and the certificate in association with the backup data package and the associated unique chip identifier.

2. (canceled)

3. (previously presented) The method as claimed in claim 1, wherein the at least one cryptographic key includes at least one cryptographic key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

4. (previously presented) The method as claimed in claim 3, wherein the at least one cryptographic key to be used for a secure, key based communication channel includes a symmetric key.

5. (original) The method as claimed in claim 4, wherein the symmetric key is generated as a function of a master key and the unique device identity.

6. (previously presented) The method as claimed in claim 3, wherein the at least one cryptographic key to be used for a secure, key based communication channel includes a private/public key pair.

7. (previously presented) The method as claimed in claim 6, wherein the private/public key pair either is:

generated by the secure processing point during assembly of the personal device; or

generated and stored in advance in a secure database before assembly of the personal device, in which latter case the cryptographic keys stored in advance of assembly are removed from the secure database after reception of the backup data package.

8. (previously presented) The method as claimed in claim 1, wherein the personal device is a wireless communications terminal and the unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network.

9. (currently amended) A system comprising:

at least one personal device, and

a secure processing point, which secure processing point is separated from and arranged in communication with the personal device,

wherein the at least one personal device includes an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper-resistant secret storage;

wherein the secure processing point includes a processor configured for retrieving the unique chip identifier and for assembling a data package and loading the data package in the personal device for storage therein, the data package including at least one cryptographic key specific to said personal device;

wherein the at least one personal device includes a processor configured for encrypting the received data package with the unique secret chip key and transferring a resulting backup data package back to the secure processing point; and

wherein the processor of the secure processing point is arranged for storing the received backup data package in association with the unique chip identifier in a permanent public database separated from the personal device;

wherein the processor of the secure processing point further is arranged for:

associating a unique device identity with the unique chip identifier;

signing the associated unique device identity and unique chip identifier~~, with~~ using a manufacturer private signature key corresponding to a manufacturer public signature key stored in a read-only memory of the personal device, thereby generating a certificate for the unique device identity;

storing the certificate in the personal device; and

storing in the permanent public database, the unique device identity and the certificate in association with the backup data package and the associated unique chip identifier.

10. (canceled)

11. (previously presented) The system as claimed in claim 9, wherein the at least one cryptographic key includes at least cryptographic one key to be used for a secure, key based communication channel between a personal device manufacturer and the personal device.

12. (previously presented) The system as claimed in claim 11, wherein the at least one cryptographic key to be used for a secure, key based communication channel includes a symmetric key.

13. (original) The system as claimed in claim 12, wherein the symmetric key is generated as a function of a master key and the unique device identity.

14. (previously presented) The system as claimed in claim 11, wherein the at least cryptographic one key to be used for a secure, key based communication channel includes a private/public key pair.

15. (previously presented) The system as claimed in claim 14, wherein the processor of the secure processing point either is:

arranged for generating the private/public key pair during assembly of the personal device; or

arranged for retrieving the private/public key pair from a secure database, in which the key pair has been stored in advance before assembly of the personal device, in which latter case the secure processing point further is arranged for removing the key pair from the secure database after reception of the backup data package.

16. (original) The system as claimed in claim 9, wherein the personal device is a wireless communications terminal and the unique device identity an identifier which identifies the wireless communications terminal in a wireless communications network.

17. (previously presented) The method of claim 1, further comprising:

reading said unique chip identifier from said read-only storage of said personal device;

transmitting the chip identifier to said permanent public database;

receiving from the permanent public database said backup data package, said backup data package corresponding to the transmitted chip identifier; and

storing the received backup data package in the personal device.

18. (currently amended) A personal device comprising:

an integrated circuit chip with a unique chip identifier in a read-only storage and a unique secret chip key in a tamper-resistant secret storage;

a processor configured for outputting the unique chip identifier; and

a memory for storing a received data package including at least one cryptographic key;

wherein the processor is further configured for encrypting the received data package with the unique secret chip key and outputting a resulting backup data package to a permanent public database separated from said personal device;

the personal device further comprising:

a read-only memory storing a manufacturer public signature key, wherein the memory for storing the received data package is further for storing a received certificate of a unique device identity, said certificate being the signing of an association of the unique device identity and the unique chip identifier ~~with~~ using a manufacturer private signature key corresponding to the manufacturer public signature key, said certificate corresponding to a certificate stored in association with the backup data package in the permanent public database and which has been signed with the manufacturer private signature key corresponding to the manufacturer public signature key.

19. (canceled)

20. (previously presented) The personal device as claimed in claim 18, wherein the at least one cryptographic key includes at least one cryptographic key to be used for

a secure, key based communication channel between a personal device manufacturer and the personal device.

21. (previously presented) The personal device as claimed in claim 20, wherein the at least one cryptographic key to be used for a secure, key based communication channel includes a symmetric key.

22. (previously presented) The personal device as claimed in claim 21, wherein the symmetric key is generated as a function of a master key and a unique device identity.

23. (previously presented) The personal device as claimed in claim 20, wherein the at least one cryptographic key to be used for a secure, key based communication channel includes a private/public key pair.

24. (previously presented) The personal device as claimed in claim 18, wherein the personal device is a wireless communications terminal and a unique device identity is an identifier which identifies the wireless communications terminal in a wireless communications network.

25. (currently amended) A secure processing point comprising:

a processor configured for:

retrieving a unique chip identifier from a read-only memory of an integrated circuit chip included in a personal device that is separated from said secure processing point;

assembling a data package and loading the data package in the personal device for storage therein, the data package including at least one cryptographic key specific to the personal device;

receiving an encrypted version of the data package, in the form of a backup data package, from the personal device in response to the stored data package;

storing the received backup data package in association with the unique chip identifier in a permanent public database separated from the personal device;

associating a unique device identity with the unique chip identifier;

signing the associated unique device identity and unique chip identifier~~, with~~ using a manufacturer private signature key corresponding to a manufacturer public signature key stored in said read-only memory of the personal device, thereby generating a certificate for the unique device identity;

storing the certificate in the personal device; and

storing in the permanent public database, the unique device identity and the certificate in association with the backup data package and the unique chip identifier.

26. (canceled)

27. (cancelled)